UNITED STATES DISTRICT COURT

for the

Eastern District of California

In the Matter of the Search of
The person of LOUIS MENDONSA and the SUBJECT PREMISES and SECOND SUBJECT PREMISES where MENDONSA stores his belongings, and any electronic devices contained therein

Case No. 2:22-sw-870-AC

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A, attached hereto and incorporated by reference.

located in the Eastern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B, attached hereto and incorporated by reference

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252(a)(2)	Distribution of Material Involving the Sexual Exploitation of Minors

The application is based on these facts:

SEE AFFIDAVIT, attached hereto and incorporated by reference.

- ☐ Continued on the attached sheet.
- ☑ Delayed notice 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Caitlan Thomas
Applicant's signature

HSI SA Caitlin Thomas
Printed name and title

Sworn to before me and signed telephonically.

Date: November 28, 2022

City and state: Sacramento, California

Allison Claire
ALLISON CLAIRE
UNITED STATES MAGISTRATE JUDGE

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND ARREST AND SEARCH WARRANTS

I, Caitlin Thomas, being duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent ("SA") with Homeland Security Investigations ("HSI") and have been so employed since April 2019. I trained at the Federal Law Enforcement Training Center and have gained experience through everyday work conducting these types of investigations. I have received training in the areas of child sexual abuse material ("CSAM") and have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I am authorized to investigate violations of the laws of the United States, including criminal violations relating to the sexual exploitation of children, child pornography, coercion and enticement, and transportation of minors, including violations of 18 U.S.C. §§ 2422, 2423, 2251, and 2252A. I have participated in investigating federal criminal violations related to high technology or cybercrime, and CSAM. Additionally, I am a member of the Sacramento Valley Internet Crimes Against Children ("ICAC") Task Force. As an SA in the Sacramento Field Office and ICAC Task Force, I frequently participate in search warrant executions involving child exploitation and pornography cases. In June 2022, I attended the National Law Enforcement Training on Child Exploitation which offered classes ranging from investigative techniques and digital forensics. Moreover, I work closely with HSI forensic examiners throughout these investigations and prosecutions.

2. I have conducted and participated in criminal investigations for violations of federal and state laws including narcotics trafficking, child sexual exploitation, money laundering, and other organized criminal activity. I have prepared, executed, and assisted in numerous search and arrest warrants. I have also conducted and participated in criminal and administrative interviews of witnesses and suspects. I am familiar with the formal methods of child exploitation investigations, including electronic surveillance, visual surveillance, general questioning of witnesses, search warrants, and the use of undercover agents. I have participated in investigations of possession, distribution, receipt, and production of CSAM.

II. PURPOSE

3. I make this Affidavit in support of an arrest warrant and Criminal Complaint charging Louis MENDONSA with violating 18 U.S.C. § 2252(a)(2), Distribution of Material Involving the Sexual Exploitation of Minors.

4. Further, I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the property located on the person of Louis MENDONSA (hereinafter referred to as the SUBJECT USER), the SUBJECT USER's property including all digital devices in or around the back corner table against the wall in the west wing of the Starbucks located at 1601 P Street, The Freemont Building, Sacramento, CA 95814 (hereinafter referred to as "SUBJECT PREMISES"), and the SUBJECT USER's property located on the porch of the residence located at 1612 18th Street, Sacramento, CA 95814 (hereinafter referred to as "SECOND SUBJECT PREMISES"), all of which are located in the Eastern District of California and more fully described in Attachment A, for the items described in Attachment B, both of which are attached and incorporated herein by reference. I submit that there is probable cause to believe that violations of 18 U.S.C. § 2252(a)(2), (b)(2) (distribution and receipt of child pornography, and attempts and conspiracies to commit such offenses) have occurred and that the evidence, fruits, contraband, and instrumentalities of those violations are located on the SUBJECT USER and at both SUBJECT PREMISES'.

5. The statements contained in this affidavit are based in part on information provided by HSI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents; information gathered from the service of administrative subpoenas; orders issued pursuant to 18 U.S.C. § 2703(d); the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by HSI agents and analysts and computer forensic professionals employed by the Department of Justice; and my experience, training and background as a SA with HSI. Because this affidavit is submitted for the limited purpose of establishing probable cause, I have not included every fact known to me concerning this

investigation. Instead, I have set forth only the facts that I believe are necessary to establish probable cause for the requested Complaint and warrants.

6. The investigation involves websites dedicated to the advertisement and distribution of CSAM on a computer network designed to facilitate anonymous communication over the Internet known as The Onion Router ("Tor") network. The investigation has revealed evidence that the SUBJECT USER is an active member of at least four such websites (Websites A through D, described below) using unique online aliases or usernames on each site,[1] and that the SUBJECT USER is distributing and facilitating the distribution of CSAM in the Eastern District of California from the SUBJECT PREMISES. Accordingly, and for the reasons set forth below, there is probable cause to believe that the SUBJECT USER traffics in, views, and possesses visual depictions of minors engaged in sexually explicit conduct, and that evidence, contraband, fruits, and instrumentalities of violations of federal statutes listed above will be found on the SUBJECT USER and at the SUBJECT PREMISES.

III. STATUTORY AUTHORITY

7. Title 18, United States Code, Section 2252 prohibits an individual from knowingly possessing, accessing with intent to view, receiving, transporting, shipping, distributing, selling, producing, and reproducing any visual depiction of, or involving, the use of a minor engaging in sexually explicit conduct, using any means or facility of interstate or foreign commerce, or shipped or transported in or affecting interstate commerce.

IV. DEFINITIONS

8. The following definitions apply to this Affidavit and its attachments:

a. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view

[1] The unique aliases/usernames are known to law enforcement but anonymized in this affidavit to protect operational security. Investigation of activity on the various websites described in this affidavit is ongoing, and disclosure of the unique aliases/usernames may alert other active users on Tor to the investigation, potentially provoking users to notify others of law enforcement action, flee, and/or destroy evidence.

postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the users who sent/received such a message, or by the bulletin board administrator.

b. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. "Chat room," as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit electronic files to other individuals within the chat room.

d. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

e. "Child pornography," as defined in 18 U.S.C. § 2256(8)(a), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or

other means, of sexually explicit conduct, where the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct.

f. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

g. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

h. The "Domain Name System" or "DNS" is a system that translates readable Internet domain names such as www.justice.gov into the numerical IP addresses of the computer server that hosts the website.

i. "Encryption" is the process of converting data into a code in order to prevent unauthorized access to the data.

j. A "hidden service," also known as an "onion service," is a website or other web service that is accessible only to users operating within the Tor anonymity network.

k. "Hyperlink" or "link" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

l. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

m. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

n. An "Internet Protocol address" or "IP address," as used herein, is a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most ISPs control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

o. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen.

p. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

q. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

r. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

s. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

t. The "Tor network" is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of relay computers, along a randomly assigned path known as a "circuit."

u. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

v. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

w. A "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

IV. RELEVANT BACKGROUND ON THE TOR NETWORK

9. The Internet is a global network of computers and other devices. Devices directly connected to the Internet are uniquely identified by IP addresses, which are used to route information between Internet-connected devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. On the Internet, data transferred between devices is split into discrete packets, each of which has two parts: a header with non-content routing and control information, such as the packet's source and destination IP addresses; and a payload, which generally contains user data or the content of a communication.

10. Websites A, B, C, and D further described below, operate on the Tor network, which is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of intermediary computers, or relays, along a randomly assigned path known as a "circuit." Because of the way the Tor network routes communications through the relay computers, traditional IP address-based identification techniques are not effective.

11. To access the Tor network, a user must install Tor software. That is most easily done by downloading the free "Tor browser" from the Tor Project, the nonprofit organization that maintains the Tor network, via their website at www.torproject.org. The Tor browser is a web browser that is configured to route a user's Internet traffic through the Tor network.

12. As with other Internet communications, a Tor user's communications are split into packets containing header information and a payload and are routed using IP addresses. For a Tor user's communications to be routed through the Tor network, a Tor user necessarily (and

voluntarily) shares the user's IP address with Tor network relay computers, which are called "nodes." The Tor user's routing information, which includes the user's destination and originating IP information, is stored in the header portion of the packet. As the packets travel through the Tor network, each node can see the address information of the previous node the communication came from and the next node the information should be sent to. Those Tor nodes are operated by volunteers – individuals or entities who have donated computers or computing power to the Tor network for it to operate.

13. Because a Tor user's communications are routed through multiple nodes before reaching their destination, when a Tor user accesses an Internet website, only the IP address of the last relay computer (the "exit node"), as opposed to the Tor user's actual IP address, appears on that website's IP address log. In addition, the content of a Tor user's communications are encrypted while the communication passes through the Tor network. That can prevent the operator of a Tor node from observing the content (but not the routing information) of other Tor users' communications.

14. The Tor Project maintains a publicly available frequently asked questions ("FAQ") page, accessible from its website, with information about the Tor network. Within the FAQ, the Tor Project advises Tor users that the first Tor relay to which a user connects can see the Tor user's actual IP address. In addition, the FAQ also cautions Tor users that the use of the Tor network does not render a user's communications totally anonymous. For example, in the Tor Project's FAQ, the question "So I'm totally anonymous if I use Tor?" is asked, to which the response is, in bold text, "No."

15. The Tor Network also enables users to operate websites, such as Websites A, B, C, and D called "hidden services" or "onion services," in a manner that attempts to conceal the true IP address of the computer hosting the website. Hidden service websites are accessible only to users operating within the Tor network. Like other websites, hidden services are hosted on computer servers that communicate through IP addresses. However, hidden services have unique technical features that attempt to conceal the computer server's location.

16. Unlike standard Internet websites, a Tor-based web address is comprised of a series of at least 16 and as many as 56 algorithm-generated characters, for example "asdlk8fs9dflku7f," followed by the suffix ".onion." Ordinarily, investigators can determine the IP address of the computer server hosting a website (such as www.justice.gov) by simply looking it up on a publicly available Domain Name System ("DNS") listing. Unlike ordinary Internet websites, however, there is no publicly available DNS listing through which one can query the IP address of a computer server that hosts a Tor hidden service. So, while law enforcement agents can often view and access hidden services that are facilitating illegal activity, they cannot determine the IP address of a Tor hidden service computer server via public lookups. Additionally, as with all Tor communications, communications between users' computers and a Tor hidden service webserver are routed through a series of intermediary computers. Accordingly, neither law enforcement nor hidden service users can use public lookups or ordinary investigative means to determine the true IP address – and therefore the location – of a computer server that hosts a hidden service.

17. Hidden service websites on the Tor Network are not "indexed" by search engines—such as Google—to anywhere near the same degree as websites that operate on the open Internet. Accordingly, it is much more difficult to perform a Google-type search of hidden service websites than it is to search open Internet websites for particular content. Users interested in accessing child exploitation material (or in advertising child exploitation and pornography websites) therefore keep, maintain, and use directory sites that advertise the web addresses of hidden services that contain child exploitation related content. Users utilize those directory sites to identify new web forums, chat sites, image galleries, and file hosts pertaining to the sexual exploitation of children.

18. Based on my training, experience, and information provided to me by other law enforcement officers, I know that users of online child pornography websites on the Tor network value their online aliases and personas as a source of bona fides within their communities. A user may attain greater status within a community of like-minded offenders over a course of time

via active participation in that community under a particular alias. That participation may amount to the trafficking of child pornography, moderation of sites, advice to users regarding safety and security, or other actions. It is therefore common for a user of one child pornography website on the Tor network to notify users of their aliases on different sites, to maintain a sort of accrued status on other sites. In fact, as described below, postings made by the SUBJECT USER on various child pornography websites on the Tor network indicate that the same user utilized multiple unique usernames across many such sites. The SUBJECT USER is believed to be the same individual operating on Websites A, B, C, and D utilizing different aliases.

V. FACTS ESTABLISHING PROBABLE CAUSE

19. As part of an ongoing child exploitation investigation, HSI Sacramento was notified of an individual who was believed to be administering[2], moderating[3], and distributing CSAM on various Tor hidden services dedicated to the sexual exploitation of children from in or around the Sacramento, California area. This Affidavit references four Tor hidden services websites, hereinafter, "Website A," "Website B," "Website C," and "Website D"; which are all dedicated to the sexual exploitation and abuse of children. [4]

20. Through ongoing undercover operations, law enforcement has monitored several dark web Tor hidden services dedicated to the sexual abuse of children, including Websites A, B,

[2] I know based on my training and experience and from speaking to other law enforcement officers that administrators of Tor hidden services are typically the individuals responsible for creating, maintaining, and operating a darknet marketplace or forum and keeping its content and design backed up and fully functional.

[3] I know based on my training and experience and from speaking to other law enforcement officers that moderators are responsible for greeting and socializing with guests, members, and staff; reviewing messages and images to ensure that they are in line with the rules of the website, and participating in staff meetings to ensure the safety and success of the website in the advertising and distributing CSAM. A Global moderator is a trusted step above, and will likely be assigned to moderate more important forum-related tasks, such as approving new members, voting on VIP members, or settling disputes between feuding members.

[4] The true names of Websites A, B, C, and D, are known to law enforcement but redacted here in order to protect the integrity of the ongoing investigation into the users of the sites.

C, and D. Based upon conversations with SAs who have experience with such investigations, I know that it is common for individuals to visit, access, or gain membership to more than one child exploitation hidden service at the same time. Through this investigation, I am familiar with Websites A, B, C, and D and know that these sites require visitors to create a username and password to access the site.

21. There is probable cause to believe the SUBJECT USER advertised and distributed CSAM on Website A as further detailed below. The SUBJECT USER is also believed to be active on Websites B, C, and D; therefore, this affidavit also addresses the SUBJECT USER'S activity on Websites B, C, and D. Law enforcement has identified the usernames believed to be used by the SUBJECT USER on Websites A, B, C, and D. The username utilized on Website A will hereinafter be referred to as "SUBJECT USERNAME 1." The username utilized on Website B will hereinafter be referred to as "SUBJECT USERNAME 2." The username utilized on Website C will hereinafter be referred to as "SUBJECT USERNAME 3." The username utilized on Website D will hereinafter be referred to as "SUBJECT USERNAME 4."[5] This Affidavit focuses primarily on the activity conducted on Websites A, B, C, and D by SUBJECT USERNAMES 1, 2, 3, and 4. Additionally, as detailed below, law enforcement has reason to believe that MENDONSA is the person who is using SUBJECT USERNAMES 1, 2, 3, and 4.

A. Investigation of Website A

[5] These usernames are known to law enforcement but redacted here to protect the integrity of the ongoing investigation into other users of Websites A, B, C, and D who may be familiar with this particular user.

Based on my training and experience, I know that users of such hidden services value their online aliases and personas as a source of bona fides within their communities. A user may attain greater status or goodwill within a community of like-minded offenders over a course of time via active participation in that community under a particular alias. That participation may amount to the trafficking of child pornography, moderation of sites, and advice to users regarding safety and security, or other actions. It is therefore common for a user of one child pornography website on the Tor network to carry an alias from one site to another, or to make other users aware that additional aliases belong to them, to maintain such accrued status or goodwill on other sites.

22. Website A is a child pornography bulletin board that facilitates the advertisement and distribution of child pornography. Since around or about January 2021, Website A has been in operation. As part of the investigation into Website A, law enforcement agents viewed, examined, and documented the contents of Website A.

23. To access postings on Website A, users are required to register a free account on the "[Website A]-Registration" page. The Registration page contains data-entry fields with the corresponding text, "Username, Password, Confirm Password, Email address, Language, My timezone." Without an actively registered member account, visitor's access to postings on Website A is restricted to the "Forum Rules" post, posted November 19, 2021. Excerpts from the "Forum Rules" include:

- *"Permitted age range for posts is 0 to 17, subject to caveats below.*
- *Banned pictures and video subjects include hurtcore*, drugged children, child is protesting (non-consensual), bullying, blackmailing & self-mutilation. Zoophilia is permitted only for 4 years old and older; the child must be "OK" with it and not be in distress.*

** Hurtcore is defined as:*

- *Anal or Vaginal penetration involving children 3 years old or younger.*
- *Any penetration causing pain regardless of age.*
- *Spanking, whipping etc. causing damage or pain*

24. After successfully registering and logging into Website A, a user can access any number of sections, forums, and sub-forums. Some of the sections and forums available to users include: "Rules," "Discussion," "Girls (Original Topics)," "Boys," and "Board Information." Additional accessible sub-forums include: "Chat," "Requests," "Hardcore," "Fetishes," "Voyeur," "Webcam/Selfie," "Studios," and "Tech Support." Some of the sub-forums, such as "Hardcore," contain the further selectable categories "Pedo (0-10 years old)" and "Hebe/Ephe (11-17 years old)."

25. In addition to forums and sub-forums containing posts, Website A includes a "the Team" page, listing trusted ranked members of Website A who administer, moderate, and contribute to the operation and continuity of the Forum. The ranked member categories listed on "the Team" page for Website A include "Administrators," "Senior Moderator," "Global Moderators," "Moderators," "Emeritus Administrators," and "Emeritus Moderators." During its investigation into Website A, law enforcement documented "the Teams" web page where SUBJECT USERNAME 1 is listed as a current "Administrator" of Website A.

26. Forum websites that require member registration, such as Website A, maintain member profile pages for each user. Member profile pages are generally viewable by all registered members of the website and contain user information including number of contributed posts, date the member joined the website, user rank (if any), member greeting signature, and the member's avatar image.

27. On November 25, 2022, I reviewed Website A, particularly the page titled, "the team," where SUBJECT USERNAME 1 is listed as one of the administrators. Upon clicking on the hyperlink for SUBJECT USERNAME 1, I was redirected to SUBJECT USERNAME 1's member profile page. This profile lists SUBJECT USERNAME 1's avatar image, website join date, number of contributed posts, last active date, and public PGP encryption key. Underneath the displayed public PGP encryption key[6] is the "User Statistics" in which I saw a website join

[6] "PGP" is also known as Pretty Good Privacy. PGP is a security program used to decrypt and encrypt messages through digital signatures and file encryptions. PGP works through a combination of cryptography, data compression, and hashing techniques. PGP uses the public key system in which every user has a unique encryption key that is known publicly in addition to a private key that only that specific user knows unless it is shared. A message is encrypted when a user sends it to someone using the recipients public key. The message is then decrypted when the recipient opens it with their private key.

The most common reason for PGP encryption use is to enable people to confidentially send messages and data to each other using a combination of their public and private keys. PGP is also used to authenticate messages and for integrity checking purposes. PGP creates a digital signature for private and public keys in order to prove that a sender is the rightful owner of the message. However, PGP can also be used to confirm that a message reaches the intended recipient.

date of December 25, 2021, a last active date of November 25, 2022, and a "Total posts" count of more than 650.

28. Here are a few examples of SUBJECT USERNAME 1's posts on Website A:

a. On July 8, 2022, at 12:44 PM UTC, SUBJECT USERNAME 1 posted an image under the topic "Girls Arcade – Chat and Share!" This post was captured by Law Enforcement on September 15, 2022. At that time, this post received 201 replies and 58,463 views. The image depicts what appears to be a prepubescent Caucasian female with dirty blonde hair wearing a pink dress with Winnie the Pooh embroidered on the front. The female is sitting on what appears to be a bed with a grayish green coloring and floral print; one leg is extended out while the other leg is bent bringing the foot inwards towards the opposite thigh. The female appears to be very small in stature in proportion to the bed she is sitting on and appears to have childlike facial features. The female's pink dress has been pulled up exposing her bare vagina and the female has no visible pubic hair. Additionally, there does not appear to be any visible body hair on the female.

b. On August 9, 2022, at 10:55 AM UTC, SUBJECT USERNAME 1 posted an image under the topic "Girls Butts." This post was captured by law enforcement on September 15, 2022. At that time, this post received 378 replies and 149,060 views. The image depicts what appears to be a prepubescent female with colorful leggings and baby blue underwear pulled down to her knees. The female has the crown of her head placed on the bed, her buttocks lifted upwards in the air, and she is bracing herself with her arms. The female's anus and vagina are exposed to the camera. The female has no visible pubic hair or body hair, and the female's hip development is consistent with that of a child. Additionally, the female appears to be small in stature in proportion to the objects around her.

c. On August 9, 2022, at 11:02 AM UTC, SUBJECT USERNAME 1 posted two images under the topic "Sucker Girls." These posts were captured by law

enforcement on September 15, 2022. At that time, these posts received 63 replies and 30,795 views. A description of the images are as follows:

i) The first image depicts what appears to be a Caucasian minor female with dark brown hair and wearing a purple shirt. There is an adult male laying down on pink bed sheets with a possible floral print. The male is wearing patterned navy underwear with a label reading, "COTTONWORLD." The adult male has his underwear pulled slightly to the side and his erect uncircumcised penis and testicles pulled out. It appears that the foreskin has been slightly pulled back exposing part of the tip of the penis as the female orally copulates the male. The male has visible pubic hair as well as significant amount of body hair on his upper legs. The female appears to be a minor as she has a youthful looking face in terms of supple skin and the female's head appears to be smaller and consistent with the size of a child's head in comparison to the male's body parts.

ii) The second image depicts what appears to be a nude prepubescent Caucasian female with brown hair. The female is kneeling on beige carpet next to what appears to be a bed with green, blue, red, and white plaid bedding and bed skirt. A heavy set, nude adult Caucasian male is standing in front of the female. The adult male has a significant amount of body hair visible on his legs and stomach in addition to pubic hair. The adult male's erect penis is penetrating the female's mouth. The female appears to be prepubescent as she no breast development and her body in comparison to the adult's body is the size of a prepubescent child.

d. On August 9, 2022, at 11:19 AM UTC, SUBJECT USERNAME 1 posted an image under the topic entitled, "The Forum Arcade." This post was captured by law enforcement on September 15, 2022. At that time, this post received 373 replies and 57,335 views. The image depicts what appears to be two pubescent females who are nude, one standing on each side of a pubescent male who is also nude. They are standing

in what appears to be a pond of water up to their knees. The females have little breast development and slightly visible pubic hair can be seen on the minor female on the left. There is very minimal hip development of the females. There is pubic hair visible on the minor male; however, the male has no visible chest or arm muscle development. Both females and the male have facial features that are consistent with a minor.

e. On August 12, 2022, at 3:05 PM UTC, SUBJECT USERNAME 1 posted an image under the topic "Sucker Girls." This post was captured by law enforcement on September 15, 2022. At that time, this post received 63 replies and 30,794 views. The image is a close-up image of an erect penis of an adult male sticking out of what appears to be the zipper opening of blue jeans. The tip of the penis is placed into the mouth of what appears to be a Caucasian minor female with dirty blonde hair. The female is holding the shaft of the penis directly below her mouth. The female's hands appear to be small and childlike and the female's face structure is very small and childlike in comparison to the male's penis and legs.

B. Investigation of Website B

29. Website B is a child pornography bulletin board that facilitates the advertisement and distribution of child pornography. Website B determined that it began operating in or about April 2022. As part of an investigation into Website B, law enforcement agents viewed, examined, and documented the contents of Website B.

30. Similarly to Website A, visitors of Website B are required to register a free user account in order to access the Forum's topics, discussions, posts, and sub-forums. After successfully registering and logging into the website, a user can access any number of sections, forums, and sub-forums. Some of the sections, forums, and sub-forums available to users include: " Rules," "Discussion," "Information," "Boy Videos," and "Boy Photos." Posts on Website B are organized as topic threads that can contain singular or multiple posts within. For example, under the "Boy Videos" - "Hard" sub-forum, there were more than 200 topics, with titles such as "Syrian Boys Fuck and Suck," "Beautiful 12yo happily fucked by man," "cum in

mouth videos – large amount," "10yo sucks again," and "Sleeping Boys Megathread (+125 videos)." Based on my training and experience, I know that "yo" refers to "years old."

31. Specially ranked members who contribute to the operation of Website B are listed on "the Team" page. The ranked member categories listed on "the Team" page for Website B include "Administrators," "Co-Admin," "Global Moderators," and "Moderators." On "the Team" page, SUBJECT USERNAME 2 is listed as a current Administrator of Website B.

32. On November 25, 2022, I reviewed Website B and its "the Team" page, where SUBJECT USERNAME 2 is listed as an administrator. Upon clicking on the hyperlink for SUBJECT USERNAME 2, I was redirected to SUBJECT USERNAME 2's member profile page. This profile page lists SUBJECT USERNAME 2's avatar image, website join date, number of contributed posts, last active date, and public PGP encryption key. Underneath the displayed public PGP encryption key is the "User Statistics" in which I saw a website join date of April 10, 2022, a last active date of November 24, 2022, and a "Total posts" count exceeding 500.

33. Next to the total topics is a hyperlink to search the user's topics. SUBJECT USERNAME 2 is associated with the following topic threads: "The Toy Factory," "[Website C]," "Artistic Photos," "TopicLinks 2.2," "Admit One Chat," "Sk8er Boys," "Freckles!," "Wigglers in B/W," "Boys Sleeping," "Profile Flair," "Artistic Beauty of Wiggles," "Loli Club Chat," "Boys Club Chat," "[Website B] Banner Contest," "Username Color Change" "[Website B] Themes," "The Levels of [Website B]," and "Board Rules."

34. Here are some examples of SUBJECT USERNAME 2's posts on Website B:

a. On November 11, 2022, at 6:37 PM UTC, SUBJECT USERNAME 2 posted an image under the topic "Boys in B/W" in the forum, "Themed Photo Topics." This post was captured by law enforcement on November 25, 2022. At that time, this post received 13 replies and 9,117 views. The image is black and white photo of what appears to be a prepubescent male who is nude and laying on his back. The male's right knee is bent with his right foot placed on the floor. The male's left leg is opened

outwards and slightly bent at the knee. The male's right hand is placed at the base of his flaccid uncircumcised penis. There is no visible pubic hair or body hair on the male. Additionally, the male lacks chest development. The male's face is also visible and appears to have childlike facial features to include supple skin. Additionally, the size of the male's penis in comparison to the size of his body is consistent with that of a prepubescent minor.

b. On November 11, 2022, at 12:04 AM UTC, SUBJECT USERNAME 2 posted an image under the topic "Group Photos of 4+ or more Boys N/NN" in the forum, "Themed Photo Topics." This post was captured by law enforcement on November 25, 2022. At that time, this post received 18 replies and 4,995 views. The image depicts what appear to be four Caucasian prepubescent males. Two of the males, who are nude, with dark brown hair are laying on their backs with their arms bent and placed behind their heads. They appear to be laying on bare twin mattresses with no covers. The third male, who is nude with light brown hair, is on his hands and knees and is orally copulating one of the males laying on their back. The fourth male, with red hair, is orally copulating the second male who is laying on his back. Due to how the photo was taken, the body of the fourth male is not visible. There is no visible pubic hair, body hair, or facial hair on the three males that are visible in the photo. Additionally, there is a lack of chest and arm muscle development in the three male's bodies that are visible in the photo. There is no visible facial hair on the fourth male. Based upon the size of the males depicted in comparison to the twin size mattresses, the males appear childlike in stature.

c. On November 11, 2022, at 12:01 AM UTC, SUBJECT USERNAME 2 posted an image under the topic "Boys Fellating Men" in the forum, "Themed Photo Topics." This post was captured by law enforcement on November 25, 2022. At that time, this post received 129 replies and 34,720 views. The image is a colored image that depicts what appears to an adult male laying on a bed with a dark colored quilt and colorful floral print design. The male's legs are spread open. There is visible body hair

on the chest, stomach, arms, armpits, and legs of the adult male. Based upon the fairness of the skin, the adult male appears to be Caucasian. Between the legs of the adult male, is what appears to be a minor male, due to the significantly smaller stature in comparison to the adult male, with light brown hair. This male is laying on his stomach and propped up slightly on his elbows. The adult's erect penis is placed in the mouth of the male. There does not appear to be visible body or facial hair on the male laying on his stomach.

35. Website B contains images uploaded by other users in which SUBJECT USERNAME 2 has access to as a member and administrator of Website B. The following is an example of a posting made by another user on Website B: on July 25, 2022, 2022, at 2:35 PM UTC, another user posted an image under the topic entitled, "Masturbating Boys." This post was captured by law enforcement on November 27, 2022. The image depicts a close-up photo of a toddler's penis. An adult male hand is gripping the shaft of the toddler's penis; the male has an olive, tan skin tone. The male's hand is significantly larger in comparison to the toddler's thigh and abdomen. Furthermore, it appears that there is a substance on and around the toddler's penis as the skin appears shiny and wet unlike the abdomen and thighs.

C. Investigation of Website C

36. Website C is a membership-based, child-pornography hidden service on the Tor network dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children. Like Websites A and B, Website C is currently operational on the Tor network. Website C's users actively post content depicting minors engaged in sexually explicit conduct and engage in online discussions involving the sexual exploitation of minors. Law enforcement's investigation of Website C determined that it began operating in or about November 2021.

37. After navigating to Website C, users are taken to a page identifying the site by name and instructing the users to complete a CAPTCHA, which is a challenge-response test used to determine whether the user attempting to visit the website is human. On or about November 25, 2022, the CAPTCHA required for entry to Website C asked users to "Click on the broken

circle to solve the captcha." Directly below those instructions was an image of what appeared to be two nude prepubescent boys laying on a bed with their penises exposed. Superimposed on this image were a series of circles, one of which was "broken" or not fully formed or connected.

38. Clicking the "broken" circle took the user to a login page for Website C, which requires users to enter a username and password to access the website. On or about November 25, 2022, a banner at the top of this page identified the name of Website C and depicted what appeared to be a nude prepubescent boy laying down, with a leaf covering his genitals. After logging into Website C, users are presented with various forums, including a forum entitled, "Videos" that contained numerous sub-forums. The sub-forms included "Movies," "Non-Nude," "Softcore," "Hardcore," "Preschool," and "Toddlers." These sub-forums contained descriptions; for example, the "Toddlers" forum description is "Boys until 3 years old." The description for the "Preschool" forum is "Boys from 3 to 5 years." Website C also contained a forum entitled, "Other" which included sub-forums entitled, "Beginners Guide," "Tech Forum," and "News and Current Information."

39. Specially ranked members who contribute to the operation of Website C are listed on "the Team" page. The ranked member categories listed on "The team" page for Website C include "Administrators," "Co-Administrator," "Senior Moderator," Global Moderators," "Forum Moderators," "Reup Doctor Chief of Staff," and "Reup Doctors."

40. On November 25, 2022, I reviewed Website C, particularly "the Team" page, where SUBJECT USERNAME 3 is listed as one of the Global Moderators. Upon clicking the hyperlink for SUBJECT USERNAME 3, I was redirected to SUBJECT USERNAME 3's member profile page. This profile page depicts SUBJECT USERNAME 3's avatar image, website join date, number of contributed posts, last active date, and public PGP encryption key. Underneath the displayed public PGP encryption key is the "User Statistics" in which I observed a website join date of January 22, 2022, a last active date of November 25, 2022, an "AoA" of 10-14, and a "Total posts" count of more than 1,600. I know from my training and experience that the abbreviation "AoA" on CSAM websites refers to "age of attraction."

41. On November 25, 2022, at 4:26 PM UTC, SUBJECT USERNAME 3 posted an image under the topic "Little ones nude [Theme]" in the forum, "Preschool." This post was captured by law enforcement on November 25, 2022. At that time, this post received 1,004 replies and 152,367 views. The colored image depicts what appears to be a prepubescent male who is nude with blonde hair. The male is laying on a bed with his arms out to his side and his right leg crossed over his left leg. The male's uncircumcised, flaccid penis is visible. The male has no visible pubic, body, or facial hair. The male lacks chest and arm muscle development. The male's facial features are childlike and the size of the male's body in comparison to the size of the bed also shows that the male's body is consistent with that of a child.

42. Website C contains images uploaded by other users in which SUBJECT USERNAME 3 has access to as a member and administrator of Website C. on November 5, 2022, at 10:27 PM UTC, another user posted an image under the topic entitled, "Black and White Photos," for which SUBJECT USERNAME 3 "thanked" the user who posted the photo. A "thank" on Website C is similar to "liking" a post on social media. This post was captured by law enforcement on November 27, 2022. The image is a black and white photo depicting what appears to be a prepubescent male who is nude laying on his back on what appears to be a couch. The male has his knees bent to his chest and feet raised towards the ceiling exposing the male's genitals. There is a lack of visible pubic hair, body hair, and facial hair. The male appears to have childlike facial features to include larger eyes and a smaller nose and mouth. There is an adult male holding the minor's leg and inserting his erect penis into the anus of the minor. This adult male has significant body hair on his legs, arms, chest, and abdomen.

D. Investigation of Website D

43. Website D is a membership-based, child-pornography hidden service on the Tor network dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children. Like Websites A, B, and C; Website D is currently operational on the Tor network. Website D users actively post content depicting minors engaged in sexually explicit conduct and engage in online discussions involving the

sexual exploitation of minors. Law enforcement's investigation of Website D determined that it began operating in or about February 2022.

44. After navigating to Website D, users are taken to a page identifying the site by name and instructing the users to complete a CAPTCHA, which is a challenge-response test used to determine whether the user attempting to visit the website is human. On or about November 25, 2022, the CAPTCHA required for entry to Website D asked users to "Click on the broken circle to solve the captcha." Directly below those instructions was an image of what appeared to be two nude, prepubescent girls laying together on a flat surface, with one girl spreading her legs and exposing her vagina. Superimposed on this image were a series of circles, one of which was "broken," or not fully formed.

45. Clicking the "broken" circle took the user to a login page for Website D, which requires users to enter a username and password to access the website. On or about November 25, 2022, a banner at the top of this page identified the name of Website D. After logging into Website D, users are presented with various forums, including a forum entitled, "Fruit" that contained numerous sub-forums. These sub-forms included "Non-Nude," "Softcore," "Hardcore," and "Webcams." These sub-forums contained instructions that the posted content should depict "4-12yo girls only." Other sub-forums in the "Fruit" forum contained similar instructions regarding the age of the minors that should be depicted in the posted content, including a sub-form titled "Young Teens," which was for "[c]ontent involving 13-17yo girls," and a sub-forum titled "Babies & Toddlers," which was for "[c]ontent involving 0-3yo girls." Website D also contained a forum entitled, "Community," which included sub-forums entitled, "Announcements & Information," "English Chat," and "Guides & Tutorials."

46. Specially ranked members who contribute to the operation of Website D are listed on "the Team" page. The ranked member categories listed on "the Team" page for Website D include, "Administrators," "Global Moderators," and "Fruit & Studios Moderators," "Stories Moderators," "Russian Moderators," "Indonesian Moderators," "Japanese Moderators," and

"French Moderators." According to the "the Team" page, SUBJECT USERNAME 4 is listed as a current Global Moderator of Website D.

47. On November 25, 2022, I reviewed Website D, particularly the page titled, "the Team," where SUBJECT USERNAME 4 is listed as one of the Global Moderators. Upon clicking on the hyperlink on SUBJECT USERNAME 4, I was redirected to a member profile page which listed the SUBJECT USERNAME 4's avatar image, website join date, number of contributed posts, last active date, and public PGP encryption key. Underneath the displayed public PGP encryption key is the "User Statistics" in which I observed a website join date of February 21, 2022, a last active date of November 25, 2022, and a "Total posts" count of more than 1,100.

48. Next to the total topics statistics, is a hyperlink to search and display the topics threads created by SUBJECT USERNAME 4. After clicking the hyperlink I observed the following topic thread titled: "Girls with Animals (NO BEASTIALITY!)," "Artistic Photography," "Black & White Photography," "Sweet Feet," Ice cream girls," "[images] Girls in an indoor pool setting," and "[Website B] – New Boy Board."

49. The following are examples of postings made by SUBJECT USERNAME 4 on Website D:

a. On November 23, 2022, at 3:54 PM UTC, SUBJECT USERNAME 4 posted an image to the topic entitled, "Latest Cum Target [THEME]," on the forum entitled, "Themed Images." This post was captured by law enforcement on November 25, 2022. At that time, this post received 890 replies and 501,798 views. The image is a colored image of what appears to be a prepubescent female who is laying on her back on the floor while nude. The female has blonde hair and what appears to be a blue bow in her hair. The female has no visible pubic hair and has chest and hip development that is consistent with a prepubescent child.

b. On November 19, 2022, at 5:29 PM UTC, SUBJECT USERNAME 4 posted an image to the topic entitled, "Girls Butt Mega Thread," on the forum entitled,

"Themed Images." This post was captured by law enforcement on November 25, 2022. At that time, this post received 893 replies and 448,246 views. The image is a colored image of what appears to be a minor female who is laying on her stomach, propped up slightly on her elbows, and looking back at the camera while nude. The female's legs are spread apart and bent at the knees exposing her buttocks and pubic area. Based upon the female's facial features, lack of body hair and pubic hair, and the small stature of the female, it appears the female is prepubescent.

c. On November 13, 2022, at 5:37 PM UTC, SUBJECT USERNAME 4 posted an image to the topic entitled, "Tween/hebe girls (Open Thread!)," on the forum entitled, "Themed Images." This post was captured by law enforcement on November 25, 2022. At that time, this post received 231 replies and 127,162 views. The image is a colored image of what appears to be a pubescent female with light brown hair who is sitting and leaning slightly backwards while nude. The female's legs are spread, and her hands are wrapped around her legs to spread the labia of her vagina exposing the vaginal opening. The female has no visible pubic or body hair; however, she does have slight breast development. Typed within the post above the image is the following: "An 11 Pic. [hyperlinked] Pedobum Album if you want more."

50. Website D contains images uploaded by other users in which SUBJECT USERNAME 4 has access to as a member and administrator of Website D. The following is an example of a posting made by another user on Website D that SUBJECT USERNAME 4 had access to: on September 11, 2022, at 4:20 AM UTC, a user posted an image under the topic entitled, "Black and White Photos" in which SUBJECT USERNAME 4 "thanked" the user on the site. This post was captured by law enforcement on November 27, 2022. The image is a black and white image of what appears to be a prepubescent female. The female is sitting on her buttocks with her knees bent, pulled towards her chest, and spread outwards. The female's pubic area is exposed to the camera. There is no visible body hair or pubic hair. The female has no breast development.

E. Basis for Law Enforcement's Belief that SUBJECT USERNAME 1, SUBJECT USERNAME 2, SUBJECT USERNAME 3, and SUBJECT USERNAME 4 are Operated by the Same Individual

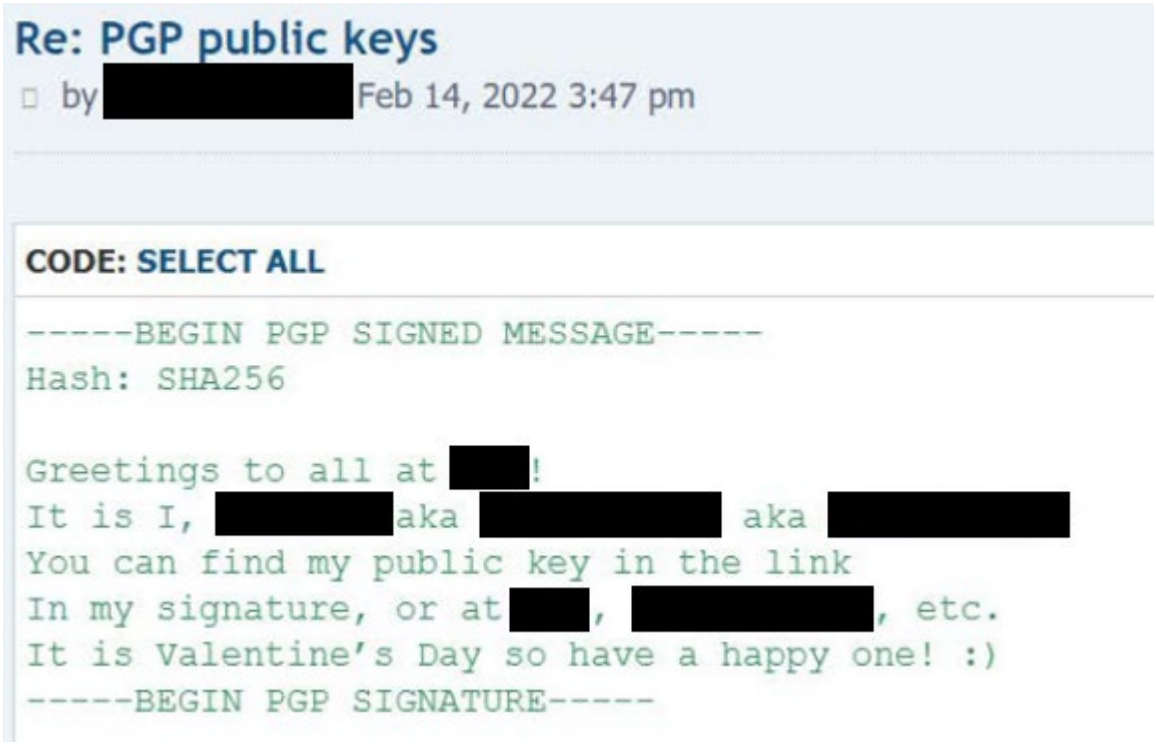
51. Through this investigation, law enforcement has reviewed multiple posts made by SUBJECT USERNAMES 1, 2, 3, and 4 where the user addresses his ownership of the separate SUBJECT USERNAME alias', linking his identity across Websites A, B, C, and D. As noted above in this affidavit, this is common for users on the dark web so that they can prove their credibility and display their duration of operation on the dark web. Below are a few examples of such posts.

52. On February 27, 2022, SUBJECT USERNAME 4 made the following post on Website D, voicing ownership of SUBJECT USERNAME 1 and SUBJECT USERNAME 2:

"Nice to meet all of you! If any of you like boys you might know me from [another Tor website known to law enforcement] and [another Tor website known to law enforcement] as PREVIOUS SUBJECT USERNAME[7], from [another Tor website known to law enforcement] as SUBJECT USERNAME 1, and currently Website B as SUBJECT USERNAME 2 . . . . Now I'm SUBJECT USERNAME 4 . . . ."

[7] The name of the PREVIOUS SUBJECT USERNAME is known to law enforcement. Investigation into the websites in which the SUBJECT USER is active on remains ongoing and disclosure of the name of this PREVIOUS SUBJECT USERNAME would potentially alert active website users to the investigation, potentially provoking users to notify other users of law enforcement action, flee, and/or destroy evidence.

53. On February 14, 2022, SUBJECT USERNAME 3 made the following post on another Tor hidden service website known to law enforcement which is dedicated to the sexual exploitation and abuse of children, that he was the same user as SUBJECT USERNAME 1, and a PREVIOUS SUBJECT USERNAME utilized on a dark web site that has since been taken down by law enforcement. Additionally, SUBJECT USERNAME 3 mentions his association with Websites A and B.

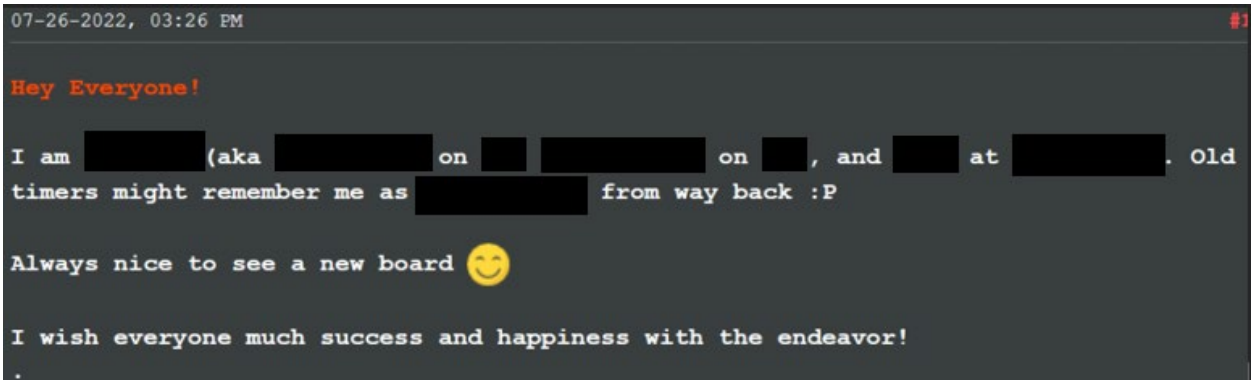


"Greetings to all at [known website]! It is I, [SUBJECT USERNAME 1] aka [SUBJECT USERNAME 3] aka [PREVIOUS SUBJECT USERNAME]. You can find my public key in the link in my signature, or at [Website B], [Website A], etc. . . ."

SUBJECT USERNAME 1's signature on this known site includes his username in a block font, a logo or mascot that appears to be associated with SUBJECT USERNAME 1, and the following reference:

"Admin @ Website A / Website B * GMod @ Website C / Website D"

54. Additional investigation revealed that an individual with this PREVIOUS SUBJECT USERNAME was an active member of other child sexual abuse material websites on the Tor network, and the same individual likely operated and continues to operate accounts and administer child sexual abuse websites under multiple claimed aliases. Law enforcement believes this to be true based upon the following post on a known child sexual abuse website on the Tor network:



"I am [SUBJECT USERNAME 1] (aka [SUBJECT USERNAME 4] on [WEBSITE D], [SUBJECT USERNAME 3] on [WEBSITE C], and [SUBJECT USERNAME 2] at [WEBSITE B]. Older timers might remember me as [PREVIOUS SUBJECT USERNAME] from way back . . . ."

F. Identification of the SUBJECT USER as Louis MENDONSA and of the SUBJECT PREMISES

55. To identify the user who was operating the PREVIOUS SUBJECT USERNAME that is linked to SUBJECT USERNAMES 1, 2, 3, and 4; law enforcement, with the assistance from analysts, conducted a search through historical user data associated with websites dedicated to the sexual exploitation of minors that were previously operational on the Tor network. The United States Department of Justice Child Exploitation & Obscenity Section ("CEOS") has been investigating users of a historical membership-based hidden service on the Tor network which operated in 2018. This was a Tor hidden service website dedicated to CSAM. Many of the users on the Tor hidden service website posted images of CSAM, requested images of CSAM, and encouraged members of the website to produce and upload images and videos of CSAM. In

March 2019, HSI SAs obtained a federal warrant to search the contents of this hidden service. After obtaining the search warrant, Fresno HSI provided a copy of the site's contents to CEOS for additional analysis. Included in the contents of the site was user registration information such as usernames, login passwords, registration dates, and number of posts. The investigation of this website identified an individual accessing the website under a moniker that the SUBJECT USER is still referencing in posts present day; therefore, in effort to protect the integrity of this ongoing investigation, this username is referred to as PREVIOUS SUBJECT USERNAME. Among the information provided was the PREVIOUS SUBJECT USERNAME's password, which was associated with a specific professional baseball team in the United States.

56. To identify the user who was operating the PREVIOUS SUBJECT USERNAME, law enforcement conducted public search engine queries for social media accounts associated with the PREVIOUS SUBJECT USERNAME. The search revealed an Instagram[8] account with an account username that was identical to that of the PREVIOUS SUBJECT USERNAME. The profile image associated with the Instagram account depicted a baseball with the name of the same professional baseball team written across the baseball as that of the password for the PREVIOUS SUBJECT USERNAME account on the hidden service that operated in 2018.

57. On or about September 22, 2022, United States Magistrate Judge Richard A. Lloret, Eastern District of Pennsylvania, issued an order pursuant to 18 U.S.C. § 2703(d) to Instagram for information associated with the account of PREVIOUS SUBJECT USERNAME with a vanity name of Louis Goodrich. On or about October 14, 2022, Instagram provided the following information regarding the following Instagram account:

> Username: [PREVIOUS SUBJECT USERNAME] (hereinafter referred to "Instagram Account A")
>
> Registered Email: [PREVIOUS SUBJECT USERNAME]@gmail.com
>
> Registration Date: 2016-05-14 03:43:51 UTC

[8] Instagram is an American photo and video sharing social networking service founded in 2010, and later acquired by Meta Platforms Inc.

58. Following the identification of this Instagram account, additional public search engine queries were conducted for the PREVIOUS SUBJECT USERNAME. An account was identified with a username of PREVIOUS SUBJECT USERNAME. The profile photo associated with the account was of a baseball with the same professional baseball team name on the ball as that of Instagram Account A. After locating this Pinterest account, additional public search engine queries were conducted, and a second Pinterest account was identified with a username consisting of a combination of SUBJECT USERNAME 1 and the PREVIOUS SUBJECT USERNAME.

59. Additionally, a Facebook account was identified with the vanity name "Louis Goodrich." This Facebook account is currently following[9] two other accounts, one of which is associated with the same professional baseball team as that of the password for the PREVIOUS SUBJECT USERNAME and as the profile photos on the Pinterest and Instagram accounts.

60. After law enforcement located the Facebook and Pinterest accounts social media accounts identified with the vanity name "Louis Goodrich," the United States sought additional 18 U.S.C. § 2703(d) orders for these accounts. On or about September 22, 2022, United States Magistrate Judge Richard A. Lloret, Eastern District of Pennsylvania, issued the orders for the Facebook and Pinterest accounts.

61. On or about October 5, 2022, Pinterest provided the following information associated with two accounts:

Username: PREVIOUS SUBJECT USERNAME (hereinafter referred to as "Pinterest Account A"

Email: [PREVIOUS SUBJECT USERNAME]@gmail.com

Created: 2016/04/14 05:14:16

[9] Users of the Facebook social media platform can choose to publicly display interests, and or be served content from accounts associated with such interests, by "following" those accounts. For example, a Facebook user interested in the San Jose Sharks hockey team may choose "follow" the San Jose Sharks hockey team account to regularly see updates and posts by that account.

Username: Combination of SUBJECT USERNAME 1 and PREVIOUS SUBJECT USERNAME (hereinafter referred to as "Pinterest Account B")

Email: [Combination of SUBJECT USERNAME 1 and PREVIOUS SUBJECT USERNAME@icloud.com]

Registration Date: 2021/12/13 14:22:06

As part of the Pinterest return for Pinterest Account B, Pinterest provided IP address 73.12.236.49, as an IP address that was accessed by the user account. On or about October 11, 2022, a Department of Homeland Security Summons was issued to Comcast for information regarding IP address 73.12.326.49, that was accessed on multiple occasions between December 13, 2021, and May 3, 2022. On November 23, 2022, Comcast responded to the summons and provided the following information regarding IP address 73.12.236.49, accessed by Pinterest Account 2. The subscriber's name was STARBUCKS-S05883 STARBUCKS with a service address of 1501 16TH St. Unit 221, Sacramento, CA 95814-6072. This is the address of "The Fremont Building," which is the apartment complex with units located above Starbucks. This is the same Starbucks coffee house with a listed address of 1601 P Street, The Fremont Bldg., Sacramento, CA 95814 (the SUBJECT PREMISES). As such, it appears the user of Pinterest Account B accessed the Internet at the SUBJECT PREMISES.

62. On or about October 14, 2022, Facebook provided the following information associated with the Facebook account of Louis Goodrich:

User ID: 100069446637159

Registered Email: [Combination of SUBJECT USERNAME 1 and PREVIOUS SUBJECT USERNAME]@icloud.com

Registration Date: 2021-06-23 06:29:43 UTC

Facebook also provided IP address history and identifying information about the Internet web browser and operating system the user appears to be utilizing to log into the account. A review of the provided information revealed the user appears to be using the Mozilla Firefox 5.0 web browser and utilizing a MacIntosh, Intel Mac OS X 10.15.

63. Law enforcement continued to conduct additional searches for the PREVIOUS SUBJECT USERNAME. In doing so, law enforcement located a CyberTipline report prepared by the National Center for Missing and Exploited Children[10] ("NCMEC") associated with the Facebook account "Louis Goodrich" with user ID 100009896286623. On April 15, 2018, NCMEC received CyberTipline Report 30815114 filed by Facebook. Facebook stated that the Louis Goodrich account with user ID 100009896286623 uploaded two (2) images of clothed minors that were classified as "apparent child pornography (unconfirmed)" on February 4, 2018. The email address associated with the reported Facebook account was [PREVIOUS SUBJECT USERNAME]@gmail.com. Facebook reported that the e-mail address had been verified. I know based on my training and experience that a verified email address indicates the user provided a valid email address and confirmed access to the email account.

64. After locating the e-mail address [PREVIOUS SUBJECT USERNAME]@gmail.com, further public search engine queries were conducted for accounts linked to that email address. A PayPal account was identified and linked to that same [PREVIOUS SUBJECT USERNAME]@gmail.com email address. After determining the linked PayPal account, additional searches on PayPal were conducted for the PREVIOUS SUBJECT USERNAME. A second PayPal account was identified as being registered to [PREVIOUS SUBJECT USERNAME]@yahoo.com.

65. After identifying both PayPal accounts, the United States sought orders pursuant to 18 U.S.C. § 2703(d) for information regarding both accounts. On or about September 22, 2022, United States Magistrate Judge Richard A. Lloret, Eastern District of Pennsylvania, issued an order for both PayPal accounts. On or about September 28, 2022, PayPal provided a consolidated response to the order and provided the following information:

Name: Louis MENDONSA

[10] NCMEC receives complaints via their CyberTipline from Internet Service Providers, Electronic Service Providers, and others. NCMEC creates reports and forwards the reports to law enforcement for further investigation.

Email Addresses: louis@calgoldenbears.com (Confirmed), [PREVIOUS SUBJECT USERNAME]@gmail.com [11](Confirmed)

Account #: 1192664714789424889

Time Created: Sat, 07 May 2016 05:39:17

Phone Numbers: 9163084285 (Confirmed), 9169952813

Addresses: 2022 10th Street, Sacramento, CA 95818 and 609 16th Street D, Sacramento, CA 95814.

66. After identifying the PREVIOUS SUBJECT USER as Louis MENDONSA, law enforcement started to investigate this individual. In or around October 2022, a search of records held by the California Department of Motor Vehicle Licensing for MENDONSA revealed the following information:

NAME: LOUIS DONALD MENDONSA

ADDRESS: 2022 10th ST, SACRAMENTO, CA 95818

SEX: M

HGT: 600

WGT: 240

HAIR: GRY

EYES: BLU

[*AGENT'S NOTE: A search of law enforcement databases revealed that MENDONSA does not appear to have ever been associated with the above noted address*.]

67. In or about October 2022, I obtained Sacramento County Department of Human Assistance Benefits Electronic Benefit Transfer ("EBT") transaction records for MENDONSA. According to the records, MENDONSA is homeless and has no cell phone. Reviewing the transactions, I noted that a majority of the EBT transactions were conducted at Peace Market

located at 1801 O St, Sacramento, CA 95811. Additionally, there were a few transactions at the Safeway located at 1814 19th St, Sacramento, CA 95811.

68. On November 2, 2022, law enforcement conducted surveillance at the Peace Market and Safeway from which MENDONSA previously purchased items. At approximately 4:25 p.m., law enforcement observed a Caucasian male matching the likeness and appearance of MENDONSA walk into Peace Market. MENDONSA was wearing what appeared to be gray sweatpants, white Nike shoes, and a black and orange hat. On November 3, 2022, I reviewed MENDONSA's EBT records and confirmed that MENDONSA utilized a welfare card to purchase items from Peace Market on November 2, 2022, at 4:26 p.m.

69. On November 4, 2022, I conducted surveillance in the vicinity of Peace Market, where MENDONSA was seen on November 2, 2022. At approximately 10:40 a.m., I saw an individual matching the likeness and appearance of MENDONSA smoking outside of the Starbucks located at 1601 P St, Sacramento[12], CA (SUBJECT PREMISES). MENDONSA was using a tablet which appeared to be an iPad. At approximately 10:50 a.m., MENDONSA was sitting in the Starbucks at a table utilizing a MacBook Pro laptop. Approximately thirty minutes later, I learned from a CEOS investigative analyst who was currently on Websites A and C and that SUBJECT USERNAMES 1 and 3 were then active on Websites A and C. At the same time, I saw that MENDONSA was using his laptop at the SUBJECT PREMISES. I could not see the laptop screen as MENDONSA positioned himself on the table in the corner of the west wing of the SUBJECT PREMISES and angled himself and the laptop away from customers. Below are two photos showing where MENDONSA was observed sitting in the SUBJECT PREMISES.

[12] This Starbucks location is the same as the SUBJECT PREMISES which matched the IP address for the Pinterest account.

70. Also on November 4, 2022, I obtained Sacramento Police Department ("SPD") Report #2012-95701 detailing that on April 9, 2012, it was reported that MENDONSA was showing pornographic images on his laptop to another individual while at a different Starbucks location. The reporting party stated the following: "I saw images of young men performing oral sex…They were clearly not for scientific purposes. The images were for sexual stimulation. Some of the images were disturbing, which included what appeared to be young boys, approximately 12 years old, with their penises exposed…" The report further detailed that SPD officers responded to the call and spoke with the reporting party. After speaking with the reporting party, SPD officers contacted MENDONSA. MENDONSA consented to a search of his computer. The SPD officers attempted to lift MENDONSA's computer from his lap, however, the power cord disconnected, and the laptop immediately shut down. While one of the officers was holding MENDONSA's computer, MENDONSA stated that he was on parole for 288 PC and that they could search him and his computer any time. That same day, MENDONSA was arrested based upon a violation of parole. MENDONSA's computer was later submitted to a forensic examiner; following review, it was determined that there was no CSAM

located on the laptop. However, the forensic examiner noted a significant amount of adult pornography. Additionally, the forensic examiner noted that CCleaner[13] software was installed on the computer and had been run on April 9, 2012, at 1728 hours. It was further noted that officers contacted MENDONSA regarding these allegations on April 9, 2012, at approximately 1747 hours. MENDONSA's Parole Agent was advised of the aforementioned facts. The Parole Agent advised that one of MENDONSA's conditions of release was that he not have any kind of pornography. As such, the adult pornography located on MENDONSA's computer was in violation of his parole.

[AGENT'S NOTE: MENDONSA was listed as a TRANSIENT during the encounter and booking of evidence on April 9, 2012.]

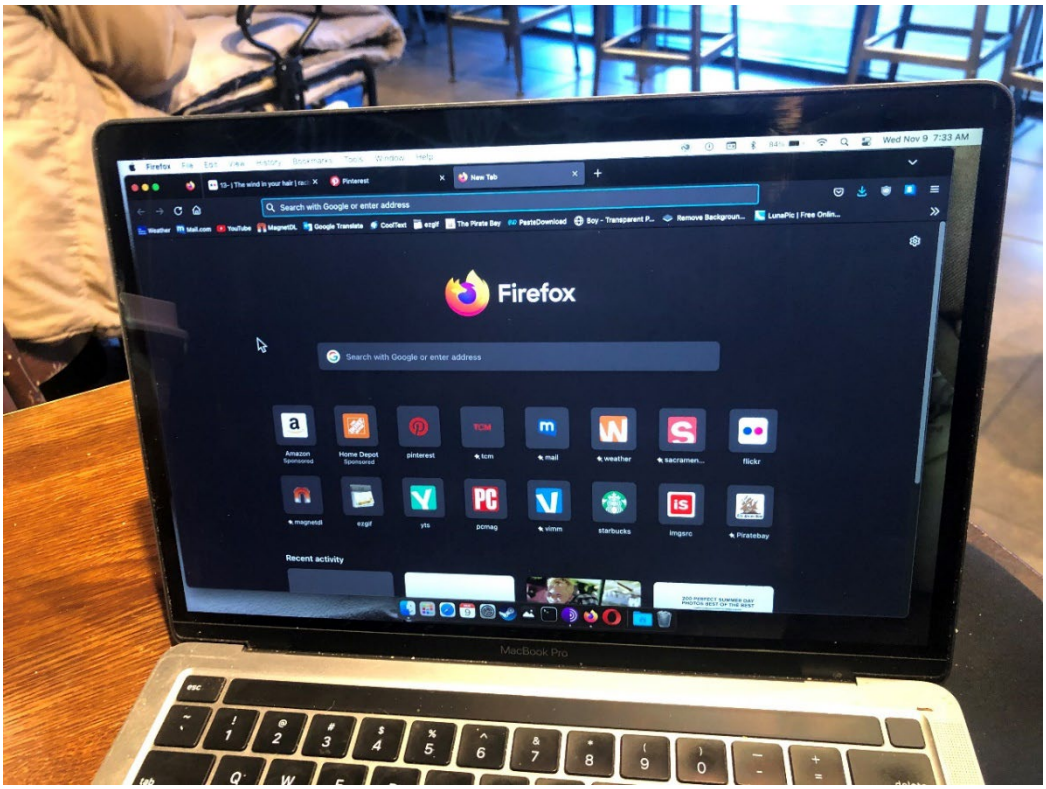
71. Law enforcement continued conducting surveillance at the same Starbucks location. Between November 6, 2022, and November 18, 2022, with the exception of November 15, 2022, MENDONSA was seen occupying the same back corner table at the SUBJECT PREMISES at approximately 6:00 a.m. nearly every day. On November 4, 2022, I saw MENDONSA at the SUBJECT PREMISES and communicated with an investigative analyst who was currently on Website C. The investigative analyst told me that the SUBJECT USER was online and active on Website C near and around the same times that I saw him on his laptop in Starbucks.

72. Similarly, on November 9, 2022, an investigative analyst who was currently on Website D told me the SUBJECT USER was online status and activity on Website D near and around the same time he was observed on his laptop in Starbucks. The investigative analyst captured the following post made by SUBJECT USERNAME 4 on November 9, 2022, on 3:47

[13] CCleaner is a software utilized to clean potentially unwanted files left by certain programs, including Internet Explorer, Firefox, Googled Chrome, Winzip, etc. along with browsing history, cookies, recycle bin, memory dumps, file fragments, log files, application data, and more. CCleaner can also uninstall programs or modify the list of programs that execute on startup. It was originally developed for Microsoft Windows only, but in 2012, a macOS version was released. Additionally, an Android version was released in 2014.

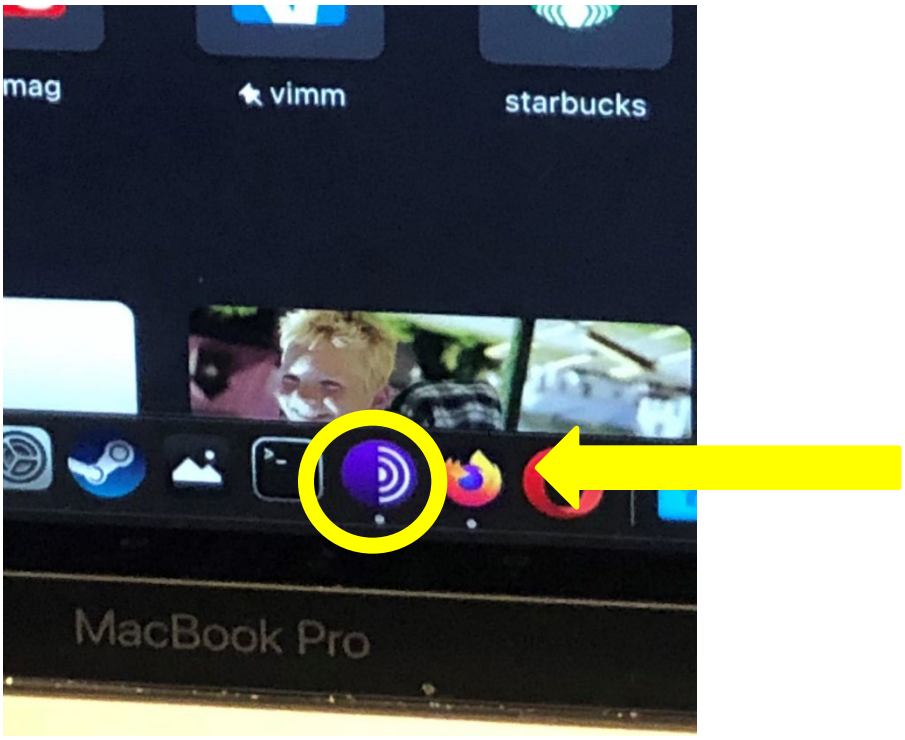
PM UTC: multiple images were posted to a topic entitled, "Daily NN picture thread," in the forum entitled, "Non-Nude Images." This post received 2,731 replies and 480,642 views at the time it was captured. These photos depict a prepubescent female with olive skin tone and light brown hair wearing a light blue two-piece swimsuit. The female is standing in the pool on what appears to be the second step and hanging on to the silver handrail. This female has no hip or breast development. Additionally, this female appears to have childlike facial features.

73. While conducting surveillance on the SUBJECT PREMISES on November 9, 2022, an HSI SA observed MENDONSA walk away from his MacBook Pro and leave his computer screen up and unlocked while he stepped outside for a smoke break. Upon closer observation, another HSI SA observed that MENDONSA had the Tor browser installed and opened as indicated by a small dot under the application which was visible on his screen. Based on my training and experience, I know that when a small dot appears under an application on Apple laptops it indicates that the specific application is open and running. The HSI SA in Starbucks near MENDONSA's computer did not toggle between the open applications to view the Tor browser. Below are two photos taken by an HSI SA depicting MENDONSA's computer on November 9, 2022. The first photo depicts the Firefox Browser open with three tabs open: Flickr, Pinterest, and the main page.



74. As shown above, multiple applications are visible on the main page of Firefox. Of note, is the icon with a red box and white letters that reads "is." Beneath this icon is the website, titled "imgsrc." I know based on my training, experience, and research that Imgsrc.ru is a free photo-sharing website based in Russia. Since at least in or about June 2012, U.S. Immigration and Customs Enforcement's ("ICE"), HSI's Cyber Crimes Center ("C3"), Child Exploitation Investigations Unit ("CEIU"), Victim Identification Program ("VIP"), as well as various international law enforcement agencies, have been investigating Imgsrc.ru as it is extensively known to be used by persons interested in exchanging images depicting CSAM to meet and become trading partners.

75. The second photo depicts a close-up of the first photo to focus on the Tor browser application on the "dock." The dot underneath the application can be seen more clearly in this photo. Also visible in this photo is an image of what appears to depict a minor male, based on male's childlike facial features.



76. MENDONSA's criminal history includes:

a. On August 10, 1993, MENDONSA was sentenced to 14 years in prison for two counts of California Penal Code (CA PC) 288(C) – LEWD/LASCIV ACTS W/ CHILD OF 14/15 and nine additional counts of CA PC 288(A) – LEWD OR LASCIV ACTS W/ CHILD UNDER 14;

b. On September 3, 2008, MENDONSA was sentenced to 32 months in prison for CA PC 290.018(b) FAIL REG W/ FEL SEX OFF/PR;

c. On April 9, 2012, MENDONSA was arrested for violation of CA PC 3056 – VIOLATION OF PAROLE. It appears that MENDONSA was subsequently released to another jurisdiction.

G. Identification of the SECOND SUBJECT PREMISES

77. While conducting surveillance on MENDONSA, law enforcement has observed MENDONSA accessing the porch area of the residence located at 1612 18th Street, Sacramento, CA 95814. On November 2, 2022, law enforcement observed MENDONSA depart the Peace Market, head south on 18th Street, and sit on a bench in front of 1612 18th Street. At

approximately 5:55 p.m., MENDONSA walked up the stairs of the residence located at 1612 18th Street. MENDONSA then retrieved other items that appeared to be a backpack and a rolled up sleeping pad from the left side of the porch. MENDONSA shortly thereafter departed this residence with what appeared to be his belongings.

78. On November 4, 2022, at approximately 12:10 p.m., I saw MENDONSA on the left side of the porch of the residence located at 1612 18th Street. Based upon the surveillance from November 2, 2022, I knew that MENDONSA stored his belongings on the porch of the residence. When I saw MENDONSA access the porch, it was unclear whether he was retrieving an item from what was believed to be his belongings or dropping off an item. After MENDONSA exited the porch, I continued surveillance on him. I saw MENDONSA depart the porch and immediately walk to the SUBJECT PREMISES. Upon confirming that MENDONSA entered back into the SUBJECT PREMISES, surveillance was concluded.

79. On November 10, 2022, law enforcement observed MENDONSA depart the SUBJECT PREMISES AT 12:17 pm and arrive at the SECOND SUBJECT PREMISES at approximately 12:22 pm. According to an HSI SA conducting surveillance inside of the Starbucks, MENDONSA returned to the SUBJECT PREMISES without his backpack.

VI. CHARACTERISTICS COMMON TO CONSUMERS OF CHILD PORNOGRAPHY

80. In conducting investigations involving child pornography and the sexual abuse of children, I have learned that individuals who create, possess, receive, distribute, advertise, or access with intent to view child pornography (collectively, "consumers" of child pornography) have a sexual interest in children and in images of children. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to such consumers of child pornography, as outlined in the following paragraphs.

81. The majority of consumers of child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

82. Consumers of child pornography may collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics, or digital or other images for their own sexual gratification. These individuals often also collect child erotica, which may consist of images or text that do not rise to the level of child pornography, but which nonetheless fuel their deviant sexual fantasies involving children. Non-pornographic, seemingly innocuous images of minors are often found on computers and digital storage devices that also contain child pornography, or that are used to communicate with others about sexual activity or interest in children. Such images are useful in attempting to identify actual minors depicted in child pornography images found during the execution of a search warrant. In certain cases, such images may also assist in determining the origins of a particular child pornography image or series of images.

83. Many consumers of child pornography maintain their sexually explicit materials for several years and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. They regularly maintain their collections in the privacy and security of their homes, inside their cars, on their person, or in cloud-based online storage. Depending on their technical expertise, access to child pornography on seemingly "safe" networks like Tor, or struggle with addiction to child pornography, many consumers of child pornography have been found to download, view, and then delete child pornography on their digital devices on a cyclical and repetitive basis.

84. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

85. Consumers of child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance, and support. This contact helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. Furthermore, individuals who would have knowledge about how to access a hidden and embedded chat site would have gained knowledge of its location through online communication with others of similar interest. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, e-mail, bulletin boards, chat sites, web forums, instant messaging applications, and other similar vehicles of communication.

86. Consumers of child pornography often collect, read, copy, or maintain names, screen names or nicknames, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange, or commercial profit. These names may be maintained in the original medium from which they were derived, in written hardcopy, on computer storage devices, or merely on scraps of paper.

87. Based upon training and experience, I know that persons engaged in the production and possession of child erotica are also often involved in the production and possession of child pornography. Likewise, I know from training and experience that persons involved in the production and possession of child pornography are often involved in the production and possession of child erotica.

88. Based on my training, knowledge, experience, and conversations with others in law enforcement, I understand that an individual who possesses images and/or videos depicting child pornography on one digital storage device and/or Internet email or online storage account is likely to possess child pornography on additional digital storage devices and/or Internet email or online storage accounts that he possesses or controls. Additionally, based on this training and experience, I understand that even if the target uses a portable device (such as a mobile phone) to

access the Internet and child pornography, it is more likely than not that evidence of this access will be found on MENDONSA's person and belongings, as set forth in Attachment A-1, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices) or on any device found on MENDONSA's person. This is true even though MENDONSA claims to be a transient. In my experience, child pornography collections are valued highly by consumers of child pornography and these images are often kept close at hand, in a location that is accessible to a consumer of child pornography. Thus, the collection, or evidence of the collection, is likely on his person.

89. Based on all of the information contained herein, I believe that MENDONSA displays characteristics common to consumers of child pornography. In particular, MENDONSA obtained and used Tor network software, acted as a staff member for Website A and Website B, acted as a general moderator for Website C and Website D, and was a member of at least four other child pornography hidden services known to law enforcement. In my experience, individuals who rely on access to materials depicting the sexual abuse of children through the Tor network tend to have sophisticated expertise with computers and they are typically individuals who are taking steps to hide their viewing of child exploitation materials.

VII. BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

90. I have had training and experience in the investigation of computer-related crimes, including those involving child pornography. Based on my training and experience, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the

camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

d. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

e. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Google, Yahoo!, and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

f. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used.

g. Some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence, suspects, victims, or other users of Website A. For example, the file data for images stored on a computer may provide geolocation information or information indicating when the file or image was created.

VIII. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

91. As described above and in Attachment B, this application seeks permission to search for records that might be found on MENDONSA's person, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

92. Based on my training, experience, and information provided by other law enforcement officers, I know that many cell phones (which are included in Attachment B's definition of "hardware") can now function essentially as small computers. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable media player, GPS navigation device, sending and receiving text messages and emails, accessing the internet, and storing a range and amount of electronic data. Examining data stored

on devices of this type can uncover, among other things, evidence of communications and evidence of communications and evidence that reveals or suggests who possessed or used the device.

93. I submit that if a computer or storage medium is found on the person of MENDONSA, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost.

b. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." An internet browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

94. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium on MENDONSA's person because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information,

records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program

to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of

Internet discussions about the crime; and other records that indicate the nature of the offense.

95. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search website all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

96. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing

logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

97. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

98. Contextual evidence establishes how computers were used, the purpose of their use, and who used them is a conclusion, based on a review of all available facts and the application of knowledge about how a computer behaves. Therefore, such evidence necessary to understand the evidence described in Attachment B is included within the scope of this warrant and will seized.

99. Further, I request judicial authorization to retain copies of all seized storage media after the review is complete, pursuant to Fed. R. Crim. P. 41 (f)(1)(B) ("The officer may retain a copy of the electronically stored information that was seized or copied.").

100. That Judicial authorization is justified in this case in part because:

a. Should the execution of the warrant uncover data that may later need to be introduced into evidence during a trial or other proceeding, the authenticity and the integrity of the evidence and the government's forensic methodology may be contested issues. Retaining copies of seized storage media may be required to prove these facts and the investigator may retain a copy of seized or electronically stored information pursuant to Fed. R. Crim. P. 41(f)(1)(B).

b. Returning the original storage medium to its owner will not allow for the preservation of that evidence. Even routine use may forever change the data it contains, alter system access times, or eliminate data stored on it.

c. Because the investigation is not yet complete, it is not possible to predict all possible defendants against whom evidence found on the storage medium might be used. That evidence might be used against persons who have no possessory interest in the storage media, or against persons yet unknown. Retention of a complete image assures that it will be available to all parties, including those known now and those later identified. Forensic analysis may identify the user names and screen names of those distributing child pornography to the user of the target computer(s).

d. The act of destroying or returning storage medium could create an opportunity for a defendant to claim, falsely, that the destroyed or returned storage medium contained evidence favorable to him. Maintaining a copy of the storage medium would permit the government, through additional warrant if necessary, to investigate such a claim.

e. Similarly, should a defendant suggest an explanation for the presence of evidence on storage medium or some defense, it may be necessary to investigate such an explanation or defense by, among other things, re-examining the storage medium with that explanation or defense in mind. This may require an additional examination of the storage medium for evidence that is described in Attachment B but was not properly identified and segregated previously.

101. I have not attempted to acquire the sought after material through any other investigative or judicial process.

102. If the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(b), the government will return these items in a reasonable amount of time not to exceed 180 days from the date of seizure unless further authorization is obtained from the Court. Due to the review team protocols described below, the examination and evaluation of seized

electronic devices is expected to take a considerable amount of time due to the limited forensic resources available.

IX. REQUEST FOR SEALING

103. Finally, I respectfully request that this Court issue an order restricting, until further order of the Court, this case, to include, the Application and Search Warrant. I believe that restricting these documents are necessary to protect the identity of cooperating individuals, because the items and information to be seized are relevant to an ongoing investigation into a criminal organization, and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal Affidavits and Search Warrants via the Internet and disseminate them to others actively seeking out information over the Web and other sources concerning law enforcement activity in this arena. Accordingly, premature disclosure of the contents of this Affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

X. CONCLUSION

104. Based on the foregoing, I submit there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits, and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located on MENDONSA and at the SUBJECT PREMISES and the SECOND SUBJECT PREMSIES, as more fully described in Attachments A-1, A-2, and A-3.

///

///

///

///

///

///

I respectfully request that this Court issue a warrant for the person and locations described in Attachment A-1, A-2, and A-3 authorizing the seizure and search of the items described in Attachment B.

I swear, under the penalty of perjury, that the foregoing information is true and correct to the best of my knowledge, information, and belief.

/s/ Caitlin Thomas

Caitlin Thomas
Special Agent
Homeland Security Investigations

Approved as to form:

Emily Sauvageau
Assistant United States Attorney

Telephonically Sworn and Subscribed to me on November 28, 2022

ALLISON CLAIRE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

PERSON TO BE SEARCHED

NAME: LOUIS DONALD MENDONSA

SEX: M

HGT: 600

WGT: 240

HAIR: GRY

EYES: BLU

ATTACHMENT A-2

LOCATION OF STARBUCKS LOCATED AT 1601 P STREET, THE FREEMONT BUILDING, SACRAMENTO, CA 95814

The belongings of MENDONSA kept in the west wing of Starbucks in or around the chair and table in which MENDONSA regularly sits and utililzes digital devices.

ATTACHMENT A-3

LOCATION OF SECOND SUBJECT RESIDENCE LOCATED AT 1612 18th STREET, SACRAMENTO, CA 95814

The porch of the residence located at 1612 18th Street in which MENDONSA has been observed on November 2, 4, and 10, 2022 leaving his belongings during the day. MENDONSA's belongings have been observed to be located on the left side of the porch.

ATTACHMENT B

ITEMS TO BE SEIZED

I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 2252 (distribution, receipt, possession, and access with intent of child pornography and the attempt and conspiracy of such offenses), and 18 U.S.C. § 2251(d) (advertisement and attempted advertisement of child pornography) (the SUBJECT OFFENSES), including:

A. Records and tangible objects pertaining to the following topics:

1. Images or visual depictions of child pornography;

2. Child erotica, including text, images, and visual depictions;

3. Communications about child pornography or sexual activity with or sexual interest in minors;

4. Internet activity reflecting a sexual interest in minors or child pornography;

5. Information concerning the minor subject of any visual depiction of child pornography, child erotica, sexual activity with other minors or adults, or of sexual interest, or that may be helpful in identifying any such minor;

6. Address books (virtual and physical), names, and lists of names and addresses of individuals who may have been contacted by use of the computer or by other means for the purpose of committing violations of the subject offenses;

7. Website A, Website B, Website C, Website D, along with all other Tor hidden services websites pertaining to the trafficking of child sexual abuse material and/or child erotica;

8. SUBJECT USERNAME 1, SUBJECT USERNAME 2, SUBJECT USERNAME 3, SUBJECT USERNAME 4, along with any other Tor username located on the seized devices;

9. Membership in online groups, clubs, or services that provide, make accessible, or otherwise concern child pornography; and

10. The existence of e-mail accounts, online storage, or other remote computer storage; Passwords or keys used to access websites and account logins

related to the conduct described herein; PGP keys and passphrases; any and all cryptocurrency and associated account information related to cryptocurrency that is related to the conduct described herein.

B. Records and tangible objects pertaining to the existence, identity, and travel of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the crimes listed above;

C. Records and tangible objects relating to the ownership, occupancy, or use of the premises to be searched (such as utility bills, phone bills, rent/mortgage payments, photographs, insurance documentation, receipts, and check registers);

D. For any computer hardware, computer software, mobile phones, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):

1. evidence of who used, owned, or controlled the computer equipment;

2. evidence of the presence or absence of malicious software that would allow others to control the items, and evidence of the presence or absence of security software designed to detect malicious software;

3. evidence of the attachment of other computer hardware or storage media;

4. evidence of counter-forensic programs (and associated data) that are designed to eliminate data;

5. evidence of how and when the computer equipment was used or accessed;

6. records of or information about any Internet Protocol addresses used;

7. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;

8. contextual information necessary to understand the evidence described in this attachment;

9. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage; and

II. All computer hardware, computer software, and storage media. Off-site searching of these items shall be limited to searching for the items described in Paragraph I.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY

AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIME.

UNITED STATES DISTRICT COURT

for the

Eastern District of California

In the Matter of the Search of
The person of LOUIS MENDONSA and the SUBJECT PREMISES and SECOND SUBJECT PREMISES where MENDONSA stores his belongings, and any electronic devices contained therein

Case No. 2:22-sw-870-AC

SEALED

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of California
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A-1, A-2, and A-3, attached hereto and incorporated by reference.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B, attached hereto and incorporated by reference.

YOU ARE COMMANDED to execute this warrant on or before December 12, 2022 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to: any authorized U.S. Magistrate Judge in the Eastern District of California.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for 30 days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: November 28, 2022 @ 3:12 p.m.

City and state: Sacramento, California

Allison Claire
ALLISON CLAIRE
UNITED STATES MAGISTRATE JUDGE

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2) (modified)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.

Subscribed, sworn to, and returned before me this date.

Signature of Judge

Date